UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/039,595	12/31/2001	Andrew F. Glew	42390.P13735	2224

7590 02/06/2007

John P. Ward, Esq.
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
FIELDS, COURTNEY D	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/06/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/039,595	**Applicant(s)** GLEW ET AL.	
	Examiner Courtney D. Fields	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 November 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1,11, and 19 have been amended.

2. Claims 1-20 are pending.

Response to Arguments

3. Applicant's arguments with respect to claim 1 have been considered but are moot in view of the new ground(s) of rejection, Potkonjak (US Patent No. 7,017,43).

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1,11, and 19 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1,11, and 19 are not limited to tangible embodiments. In view of Applicant's disclosure, specification page 7, lines 5-17, page 13, lines 2-5 and page 11, lines 13-21. With regards to claim 1, the code module and the machine readable medium is not limited to tangible embodiments, instead being defined as including both tangible embodiments (i.e. disk or memory storage device) and intangible embodiments (i.e., software program per se). A computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process. Computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer which permit the computer program's functionality to be realized. When nonfunctional descriptive material is recorded on some computer-readable or machine-readable medium, in a computer, on a data structure, or on an

electromagnetic carrier signal, it is not statutory. As such, claims 1,11, and 19 are not limited to statutory subject matter and is therefore non-statutory.

6. A computer program per se and a machine-readable medium stored on a data structure do not fall within one of the four statutory categories of the invention, (i.e., process, machine, compositions of matter, and manufacture).

7. Furthermore, the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of § 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*. .

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al. (US Patent No. 6,401,208) in view of Potkonjak (US Patent No. 7,017,43).

Referring to the rejection of claims 1 and 11, Davis et al. teaches and discloses a technique for verifying if the BIOS code has been illicitly modified, by using a pre-programming cryptographic device. The cryptographic device contains BIOS code, a BIOS certificate and a BIOS signature. The BIOS signature is decrypted with the certificate key. BIOS signature is retrieved from the BIOS cryptographic device by decrypting the BIOS certificate using a root certification key, retrieving a public key from the BIOS signature and using the public key to recover a pre-loaded digest. (See Davis et al., Column 5, lines 4-67, Column 6, lines 1-13)

However, Davis et al. does not teach decrypting the signature using a key embedded in a chipset of the computing device.

Potkonjak teaches and discloses a cryptographic technique for identification or a signature or message embedded within a integrated circuit, wherein after selecting the encoding scheme for the signature data, the encoded signature data is enciphered and then embedded. This provides at least two advantages. First, it strengthens the proof of authorship by allowing only the holder of the secret key to decipher the signature data. Next, it makes the signature data look like a random bitstream so that the detection of the signature data by unauthorized users using any statistical analysis becomes more difficult. (See Potkonjak, Column 16, lines 65-67, Column 17, lines 1-20)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Davis et al.'s method for authenticating BIOS code with Potkonjak's integrated circuit identification system. Motivation for such an implementation would enable an identifier to be detected by observing the relationship between input data and output data of a device, such as an integrated circuit. The encrypted identifier located in intellectual property, such as in an integrated circuit, may be decrypted using a key, wherein the key identifies an authorized recipient (See Potkonjak, Column 2, lines 17-27)

Referring to the rejection of claims 2 and 12, (Davis et al. as modified) discloses the claimed limitation wherein the signature further attests to the authenticity of the data (See Davis et al., Column 2, lines 64-66)

Referring to the rejection of claims 3, (Davis et al. as modified) discloses the claimed limitation wherein the signature comprises a digest value computed from the code and the data (See Davis et al., Column 2,lines 56-61)

Referring to the rejection of claims 4,13, and 20, (Davis et al. as modified) discloses the claimed limitation wherein after recovering a pre-loaded digest, the BIOS code undergoes a one-way hash (SHA -1 hash) function to produce a resultant digest. If there is a match, the BIOS code becomes authenticated. (See Davis et al., Column 5, lines 66-67, Column 6, lines 1-19) The one-way hash derives from the Digital Signature Standard, which converts the information of a variable-length into information of a fixed length (i.e., digest) (See Davis et al., Column 2, lines 46-64)

Referring to the rejection of claims 5, (Davis et al. as modified) discloses the claimed limitation wherein the signature comprises a hash of the code and the data (See Davis et al., Column 2, lines 53-67, Column 6, line 1)

Referring to the rejection of claims 6 and 14, (Davis et al. as modified) discloses the claimed limitation wherein identifying when execution of BIOS code should be prevented or accessible by authenticating BIOS code using a cryptographic device as a means for computing. (See Davis et al., Column 5, lines 9-32)

Referring to the rejection of claims 7 and 15, (Davis et al. as modified) discloses the claimed limitation wherein once the BIOS code has been authenticated, the cryptographic device generates a predetermined signal (marker) of code, in order to begin and end execution. Once the instructions have been fetched to the vector, the BIOS code becomes authenticated. (See Davis et al., Column 6, lines 20-30) As defined in the Applicant's Specification, on page 13, lines 9-12, a marker comprising a predefined bit pattern that signals the end of the code pages and data pages. Therefore, the predetermined signal is equivalent to the marker of code.

Referring to the rejection of claims 8 and 16, (Davis et al. as modified) discloses the claimed limitation wherein the cryptographic engine which performs encryption and decryption as DES-based or RSA based (i.e., encryption algorithms). The chipset contains code modules such as BIOS code for performing cryptographic functions within the IC devices (See Davis et al., Column 3, lines 31-40, Column 4, lines 21-40)

Referring to the rejection of claims 9 and 17, (Davis et al. as modified) discloses the claimed limitation wherein a field that specifies an execution point of a post-code module from which the computing device initiates execution of the post-code module after executing the code module (See Davis et al., Column 5, lines 4-31)

Referring to the rejection of claims 10 and 18, (Davis et al. as modified) discloses the claimed limitation wherein the code comprises a terminate instruction that specifies an execution point of a post code module and that in response to being executed results in the computing device terminating execution of the code module and initiating execution of the post-code module from the execution point (See Davis et al., Column 5, lines 32-67, Column 6, lines 1-13)

Referring to the rejection of claim 19, (Davis et al. as modified) discloses a machine readable medium comprising: data pages comprising data, code pages comprising code to be executed by a computing device and a value that fingerprints the data pages and the code pages (See Davis et al., Column 5, lines 66-67, Column 6, lines 1-13)

However, Davis et al. does not teach decrypting the value using an asymmetric key embedded in a hardware component of the computing device.

Potkonjak teaches and discloses a cryptographic technique for identification or a signature or message embedded within a integrated circuit, wherein after selecting the encoding scheme for the signature data, the encoded signature data is enciphered and then embedded. This provides at least two advantages. First, it strengthens the proof of authorship by allowing only the holder of the secret key to decipher the signature data. Next, it makes the signature data look like a random bitstream so that the detection of the signature data by unauthorized users using any statistical analysis becomes more difficult. (See Potkonjak, Column 16, lines 65-67, Column 17, lines 1-20)

Potkonjak teaches and discloses decrypting the value using an asymmetric key (public key/private key) embedded in the circuit design of the computing device (See Column 2, lines 12-27)

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Davis et al.'s method for authenticating BIOS code with Potkonjak's integrated circuit identification system. Motivation for such an implementation would enable an identifier to be detected by observing the relationship between input data and output data of a device, such as an integrated circuit. The encrypted identifier located in intellectual property, such as in an integrated circuit, may be decrypted using a key, wherein the key identifies an authorized recipient (See Potkonjak, Column 2, lines 17-27)

Regarding claim 20, (Davis et al. as modified) discloses the claimed limitation wherein the value is encrypted via the RSA encryption algorithm and an asymmetric key paired with the asymmetric key of the hardware component and the value comprises a SHA-1 hash of the data pages and the code pages (See Davis et al., Column 4, lines 29-40)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cdf
February 1, 2007

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER